DEPARTMENT OF DEFENSE BLOGGERS ROUNDTABLE WITH COLONEL WAYNE PARKS, DIRECTOR, COMPUTER NETWORK OPERATIONS-ELECTRONIC WARFARE PROPONENT; LIEUTENANT COLONEL FRED HARPER, DEPUTY DIRECTOR FOR REQUIREMENTS VIA TELECONFERENCE FROM FORT LEAVENWORTH, KANSAS TIME: 10:00 A.M. EDT DATE: TUESDAY, AUGUST 5, 2008

(Note: Please refer to www.dod.mil for more information.)

LIEUTENANT JENNIFER CRAGG (Office of the Secretary of Defense for Public Affairs): Jack is out today, so I'm going to go ahead and start with the call, sir, if you're ready. And then I'll turn it over to you in a couple seconds.

COL. PARKS: Okay.

LT. CRAGG: Okay. With that, hello, I'd like to welcome you all to the Department of Defense's Bloggers Roundtable for Tuesday, August 5th, 2008. My name is Lieutenant Jennifer Cragg with the Office of the Secretary of Defense for Public Affairs and I'll be moderating this call today.

A note to the bloggers on the line: Please state your name and the organization that you are with. Today our guests are Colonel Wayne Parks and Lieutenant Colonel Fred Harper. Colonel Parks is the director of Computer Network Operations-Electronic Warfare Proponent and TRADOC capabilities manager for Electronic Warfare Integration at the Combined Arms Center, Fort Leavenworth, Kansas.

Sir, with that I'm going to turn it over to you for opening statement and then we'll go right into the questions.

COL. PARKS: Okay, thanks. Well, welcome and good morning. We appreciate another opportunity here at Fort Leavenworth to come on a Bloggers Roundtable. I got a tremendous amount of -- personally and professionally a tremendous amount of information in exchange last time. And it's been very helpful for us as we've headed down the path over the last several months to continue our development efforts.

Those of you that remember or maybe not remember this past April, you gave us here at the Combined Arms Center in Fort Leavenworth the opportunity to address this forum on the topic of information and cyberspace, which are highly interrelated but also distinct in what they bring to full-spectrum operations. There are some distinct differences. The discussion was wide-ranging and we addressed the ways in which we're attempting to conceptualize operations in cyberspace so that we can be effective and successful and how our Army's changing radically to account for the increasingly wired and wireless world.

I confessed at the time that we were still wrestling with definitions and roles and responsibilities. I'm happy to report we've made some headway over the past four months. I think my folks would probably like me to say significant headway, but I wouldn't say that yet. But we have made some headway in definitely moving and leaping into the right direction.

Today what I'd like to do is focus squarely on two topics which are the core of this proponent's mission. One is understanding cyberelectronics that is -- it is evolving in our thinking, and two, appreciating the current state of our development efforts, particularly on the electronic warfare front. That's what I brought Colonel -- Lieutenant Colonel Harper on line today for, is, he -- he takes the lead from me on the area of electronic warfare. And there's been some tremendous things going on, especially in OEF and OIF, where electronic warfare has helped in the operations and in limiting and reducing what I -- reducing the deaths in theater.

Although perhaps a bit simplistic, cyberelectronics, specifically cyberspace, correlates to the medium or infrastructure though which data is transported. But there's a significant difference, to a large extent, with the science behind our (understanding ?) of what we're calling the cyberelectronic dimension -- relates to the area of the natural, formal and computer sciences. Our understanding of the science of cyberelectronics is relatively immature at this point. It includes the study of both the physical and the virtual, which caused us to reach out to academia and industry in our development efforts, which we talked a little bit about last time.

Cyberelectronics includes more than what we may be defining as cyberspace and involves what we call the broader electromagnetic spectrum.

The official title of the proponent is the CNO, Computer Network Operations, and the EW, Electronic Warfare Proponent, as if they're separate and distinct. Part of our task is to ensure that the Army works through these concepts carefully and defines them in such a way that we don't limit our intellectual exploration of potential and emerging concepts or capabilities.

Cyberelectronics could include or have distinct relationships between things that we call network operations, network warfare, computer network operations, space superiority, electronic warfare and the electromagnetic spectrum operations. Each represents a different   slice of the cyberelectronic continuum within which different capabilities must exist. We will focus today on -- in our discussion on cyberelectronics and how it could contribute to full-spectrum operations in terms of what I've just described.

Of these pieces we have talked about, the one we've focused on intently over the past few years has been electronic warfare. Operational requirements in OIF and OEF, especially the defeat of IEDs, spurred the Army to speed development of near-term solutions such as EW leader and practitioner development courses, mobile training teams and the crew system.

Even as we've sped toward these near-term solutions to the field, though, we've been simultaneously developing EW concepts for the mid- to long term through the formal capabilities base assessment process. That's what we call our long-term process that aligns with the planning program and budgeting processes.

The process essentially identifies gaps that exist between anticipated requirements and current capabilities and the means to bridge these gaps, that

EWCBA will be completed this December and at the same time we'll have Field Manual 3-36, Electronic Warfare Operations," published. These efforts -- they're having a great impact on operations in OEF and OIF, as we understand it today.

On the CNO front, we'll be hosting a cyberspace symposium in late September.

Again, we had one back in May, and we'll be doing it again in September. It'll also serve as a launch pad for the cyberelectronic operational concepts, or at least the conceptual thinking. And the first step towards identifying cyberelectronic gaps and solutions.

Okay, with that being said,, that's a broad overview of what I hope we could do today in -- to help frame your questions. And so I'll let you go ahead and fire away at us.

LT. CRAGG: Thank you, sir, for that introduction. We have three callers on the line now. Did anybody else join us?

Q Colin Clark here.

LT. CRAGG: Colin Clark? Okay, great.

So let's go ahead and start with Andrew. Andrew, go ahead.

Q Thank you. Colonel, Andrew Lubin from U.S. Naval Institute's Proceedings and Get the Gouge. I appreciate you taking the time to speak with us again, sir.

Okay, Colonel, The New York Times yesterday and the day before reported that Mullah Omar, from -- you know, from 9/11, and Osama bin Laden actually is running al Qaeda from Quetta and has his own website that talks -- that -- in Arabic, that discusses their entire range of -- (inaudible) -- the Afghan shadow government. Do you have any sort of way to reach into the Arabic world and to start doing -- and start getting information out and to them?

COL. PARKS: Reach into the Arabic world and -- you're saying get information to them or get information from them?

Q Combination of both, actually. I mean, I figure if it's on the Web, it's free-range. But if there's a lot of people in Afghanistan and Central Asia looking at the Web in Dari, Pashtu or Arabic, are we involved in there also? Are they getting our story, or are they just getting Mullah Omar's story?

COL. PARKS: Well, this is actually a little bit out of my field. We have an Information Operations Proponent, and the last time you spoke to me, I was the interim director for that.

Q Right. COL. PARKS: I'm no longer the interim director. That's a guy named Colonel Dave Haught now.

Q Okay.

COL. PARKS: And the question you're asking me is more along the lines of inform and influence, or what we call information engagement. I'll tell you what I know, but I'd be speaking for Dave. And that is, is that we're doing quite a bit, both on the ground -- which is obviously what we have done with our surges -- surge in Iraq and then, as we're looking at the situation in Afghanistan and attempting to put the appropriate types and numbers of people on the ground there who, with our multinational partners -- yes, you know, we're distinctly engaged and deeply engaged with our partners over there in the -- as you call it, the Arabic world.

The other thing too is if you look in the area of cyberspace, yes, we're doing everything that's possible with monitoring the 'net, whatever that might mean. You know, there's all kinds of ways to monitor the 'net in different locations. We'll stick pretty strictly to the Internet here in order to see what is going on and to be able to directly engage with folks in that part of the world and get at, I think, what you're talking about.

Q   Okay. Thank you.

LT. CRAGG: Okay. Let's go to the next caller.

Richard?

Q   Hello. This is Richard Lowry with op-for.com. Colonel, could you comment on the issue of cyberforce protection versus national defense?

While it's vital that we protect our military networks, the government's charter is to provide for the common defense. How do you envision protecting commercial cyberinfrastructure in the future?

COL. PARKS: Right. You know, much of the conversation we've been in for cyberspace, since I've been on the job, has been on protecting the nation's infrastructure and the nation's networks. Of course, as an army, we have a couple of responsibilities. One is -- certainly is, as we're asked to deploy around the world and be in the active force or on the active side, the active force has a significant responsibility to deploy around the world and operate there. So what that causes us to do is to figure out how to protect our own internal capabilities and networks and forth.

At the same time, is -- we do have this responsibility to provide a defense around our borders or inside our borders. The problem here that we're talking about is there's not really distinct borders in the area we're talking about. But as you're alluding to is -- areas of the financial industry in the United States, the travel industry, all those things that are on the Internet and operating through cyberelectronics, we're working very hard with our partners in the interagency to determine how we do that, even to the point where we're having discussions about the U.S. code all the way from code -- from the article six to 10 to 18 to 32 to 40 to 50. All of those different codes give us roles and responsibilities and authorities for who is to protect the nation in certain ways and manners.

And so what we're doing is -- with our interagency partners -- is determining how does the U.S. military or the Department of Defense perform their mission at a national level in protecting the borders of the United States as well as our responsibility to deploy around the world and be able to protect the United States from distant locations.

Q   Thank you. It's truly a brave new world, with technology.

COL. PARKS: Absolutely. And as I'd mentioned earlier, the problem that -- trying to get people to understand here is that there is no nation-state border where we're talking now. There are nation- state sponsors and we have to look at it in terms of a nation-state sponsor as well as those who are not nation-state sponsors -- I might call them cyberstate sponsors -- who are really developing on their own out there. And there's nothing that -- across the world that really rules or governs that to a certain degree. A lot more study in how international law and national law and local law impacts all of what we're talking about and digging really deep into that. And as you may have seen in my opening statement and the last time I talked about -- we're reaching out to the world of academia and industry here at Fort Leavenworth in the Combined Arms Center fairly significantly here throughout the Great Plains, the Big 12, others here in order to really get at this problem and get the intellectual capacity to deal with this, versus just inside the Army trying to figure this out, because to a large degree, we don't have that kind of expertise.

Q   Thank you.

LT. CRAGG: Okay. Let's go on to Grim, please.

Q   Hey. This is Grim of Blackfive.net. Colonel, I would like to ask you about the impact of cyberspace on recruitment for, for example, foreign fighters coming into Iraq. We know that there haven't been that many of them compared to the total number of insurgents, but they've been a majority, for example, of suicide bombers. So they're an important factor.

To what degree is cyberspace a major influence on recruitment, or does it depend more on physical networks of families, friends, social groups, that sort of thing? And also, do you think that cyberspace serves as -- to sort of drag people into those physical groups, or is it in fact important in its own right?

COL. PARKS: Well, again, this is in the area of what I would call the information operations proponent and what they do, because you're now talking about the cognitive, humanity, social sciences of our business in full-spectrum operations in the Army. And so you're really getting into the minds of people.

What my proponent is more focused in is building capabilities in those areas of the natural and the formal sciences and computer sciences.

Now, it does enable the information operations proponent in doing what they do. But really what I'm trying to talk about today is, is more along the lines of how do we build capability to deal with things -- like in the Army we've got the Future Combat System. We got a thing called LandWarNet. You've got other nations out there who are building those same types of capabilities. And interestingly enough, there's not just the human-to-human contact; there's the machine-to- machine, robotic-to-robotic, some virtual worlds that are popping up out there, which are not necessarily -- just have humans involved.

So I could answer that question like I did the one before, but I really am treading on somebody else's business. And what I'm trying to get folks to understand is, this is beyond just information engagement from human to human.

Simple answer to your question there is, is yes. All of what you described is happening out there. All of what you described is, is my   buddy downstairs spends a lot of time with communities out there, understanding, again, the cognitive, the humanities, the social sciences aspects and trying to figure out how do you inform and influence folks to act and react in a way that ideally brings peace back to the areas that we've become engaged with.

Q All right. Well, in that case, would you like to talk a bit about the popping up of virtual worlds that you mentioned a minute ago, because that sounds like something we might want to know more about.

COL. PARKS: Yeah, that's not a bad idea, because that is one of -- an area that, as we're starting to talk to folks and really starting to dig into this intellectual piece, is that there's really not a lot of discussion about the what you're calling virtual world. There's a lot of different names for it, but really a cyberworld that's out there, in some cases which is acting on its own in a machine and not necessarily -- and it is influencing and impacting what the human's doing, but it's not necessarily human-to-human contact.

Do you have a specific question?

Q No. I'm not as well-informed as you are on this subject, so I'd just like to hear more of a briefing as to where you think these things are coming up and what sorts of threats or opportunities they pose for us.

COL. PARKS: I was at one of the local universities here the other day and watching what some of the youngsters were talking -- I think they were all graduate students, but, you know, they're in their early 20s, are coming up with as far as projects in the area of what I'm calling cyberelectronics, or some might call cyberspace. And there's a myriad of terms for it, but one is it's like self-healing networks.

There are these virtual worlds out there that if a piece of that network were to go down, the system itself in and of itself will find out where that system went down, find out where that weak point is, and it actually has a way to regenerate and/or to repair that particular node or particular place, and it's a self-healing type of capability.

So the ability to go out and attack a network in the future, or even maybe today -- I don't necessarily know how advanced this is, but it's certainly in the future -- is you can attack it all you want, but if it's no longer relying upon the human to repair and it's got a self-healing capability of its own, that thing will heal itself in just, you know, microseconds in some cases and things will continue to operate.

So, for example, something that may be controlling an unmanned aerial system somewhere will have a self-healing capability, so if I try to interject that signal, it's going to probably come right back up and I'm going to have to have a way continually to engage that if I really want to affect that type of system. And when I say unmanned aerial system, I don't know if you could call that a robot or not, but in some cases you set that unmanned aerial system now to fly a pattern and to actually program some things in for it to make its own decisions, and it will go places it needs to go without you ever having to interject the system.

Q Well, self-healing was the concept behind the Internet to begin with, that it could route around damage. Are you talking about something that's more robust, or is this really a different, new concept?

COL. PARKS: I would say, yes, the answer's more robust and a new concept. You know, again, in an internet, you're talking about a self-healing capability that allows the communications to continue on. This is getting more along the lines of a -- and I'm going to have to think about the term.

Before we're done here, I'll think of that term and I'll be able to get it to you. But I can't remember what it's called right now.

LT. CRAGG: Let's go ahead and go with another caller on the line, Colin. And did anybody else join us after Colin?

Q No, that was Colin coming back after he had problems.

LT. CRAGG: Okay. Colin, go ahead and shoot with your questions.

Q Colonel, first I want to ask your opinion of Lieutenant Colonel John Coui (ph). I can guess. Second, I wondered if you could talk a bit about the FCS network and the work I know you guys have had to do with (GSA ?) and the other joint offices to get all this to work.

COL. PARKS: Well, FCS, in and of itself, that's not my responsibility. But I'll tell you what I know, but --

Q Understood. I'm only talking about the net part.

COL. PARKS: Yeah, the area of cyberelectronics. The Future Combat System, as you well know, is intended to be a networked system that is going to be able to operate across the globe, distributed capabilities -- (inaudible) -- missions. And what we're doing is we're engaged with the FCS community.

One is to determine how to protect it. It becomes a significant center of gravity for us, once that network's up and running in those different nodes. And I'll call them nodes out there. A node could be a vehicle. A node could be a particular weapons system or component on a vehicle inside a vehicle. It could a component or a proponent inside the pocket of a soldier or trooper, or it could be the communications that allows the humans to interact with each other for what we call battle command on our Future Combat System. So the need to be able to protect that is pretty immense.

It's got -- obviously, in the physics of it, it's got a series of wireless and wired capabilities depending upon, you know, where we're at. You know, I don't know if vehicles, for example, are going to go wireless inside a vehicle, but that's an interesting thought, as we're -- is it easier and better to have wireless components versus thousands of miles of wires running through an Apache helicopter, reduce weight? Those kinds of things are popping up. And so we're having to take a look -- is how would I protect that, if that happened, from being attacked?

On the other hand is those Future Combat Systems could have the capability of having weapons systems on board that are cyber-type weapons systems. Example: In the area of electronic warfare, things like acoustics, things like -- help me out here, Fred -- laser. The other day we were talking about just laser communications alone, being able to link to communications systems off of a laser transmission. Those are the kinds of things we're building into our systems now that you might be able to attack the adversary and so in -- attack and defense all rolled up into one in our Future Combat Systems in the area of what we're calling cyberelectronics.

Q   Okay. And how smoothly or not are the coordination pieces going with DISA and the other joint pieces?

COL. PARKS: Well, I'd say, as smoothly as you could ever hope to have happen, at this point, you know.

Q   So it's that bad. (Laughs.)

COL. PARKS: Well, just a second, and I'll get you an answer for that.

For example is that here at the Combined Arms Center, one of the things that General Caldwell has impressed upon us, and that we're doing very well, is the collaboration from inception versus waiting until the Army gets a system out there and approved, to go work with your sister services as they get things approved. And that would also include places like DISA and other interagency-type organizations. But in the Department of Defense, it would include DISA.

So the Air Combat Command, for example, NAVWARCOM -- (inaudible) -- for the Marine Corps and the Combined Arms Center and TRADOC here at Fort Leavenworth, working together from inception. Our symposium that's coming up in September for example will have representatives from all those different organizations.

It will have representatives from STRATCOM, Joint Forces Command that they have. And they've got a series of those, one of which is Joint Task Force-Global Network Operations, which is actually a DISA organization working for STRATCOM. Or you might say it's a STRATCOM organization working for DISA. And I can't off the top of my head remember the command-and-control relationship. But you have the DISA commander responsible for that joint task force and what it does.

So with that being said, that's a pretty strong relationship, when you think about it, in getting at the integration and collaboration from inception versus waiting until we get way down the road, in capability development, before they all come together.

Q   I'm sorry, sir, if you said it, I couldn't hear it. What's the topic of this meeting coming up?

COL. PARKS: It's what we have termed, in the past, the Information in Cyberspace Symposium. This is our second iteration of the Information in Cyberspace Symposium. And on the cyberspace side,   which is my area of responsibility, we're focused on what we're calling the development of cyberelectronic concepts.

Q   Thanks.

LT. CRAGG: If we can go around the horn, we have a couple minutes just for a last few quick questions.

Q   Yeah, I've got a follow-up.

LT. CRAGG: Okay.

Q   Yeah, Colonel. Andrew Lubin again.

You were talking earlier about the networks that are self-healing or self-regenerating. Are you still seeing a lot -- we read about these sporadically -- in the way of Chinese, Russian, Ukrainian attacks on the Pentagon and on the American military system?

COL. PARKS: I'll just go with what's obviously in the open press here, given the venue we're talking. But recent issues associated with what's going on in the Pentagon, I can't talk to directly.

I don't necessarily know I have the in-depth knowledge to do that. But across the board, all different types of attacks coming on the U.S. from across the globe. And as we mentioned earlier, is we're deeply engaged with the interagency throughout the administration trying to determine what those attacks are, where they're coming from, who's really responsible for them. And in my case, my responsibility is to try to determine the types of capabilities that the Army can provide, both to the Joint Force and to the interagency to be able to defend against that.

Q   Okay. Thank you.

LT. CRAGG: Anybody, last-minute question?

COL. PARKS: If I could, what I'd like to do is if somebody has a question on the area of electronic warfare, again, I have the expert in the room here on what we've done over the last few years. And I would highlight that in the area of radio-controlled improvised explosive devices, as the Army over the last two to three years has put capability into the field, those numbers have gone down significantly, and the U.S. deaths, especially in Iraq, have gone down significantly. And much of it, we believe -- I don't have the science behind it at this point, but we certainly believe is towards those types of -- the type of education, training and types of materiel being put into the field in the hands of soldiers.

Q   I have a quick question. Have you done anything to counter IR triggers for IEDs?

COL. PARKS: I'm going to turn this over to Colonel -- Lieutenant Colonel Fred Harper for a second to answer your question.

LT. COL. HARPER: Good morning.

Yes, there has been some work done in that area, primarily the actual triggering of the device. Although I can't get into specifics, there is some work that is being done, and a lot of training to counter those type of techniques that are being used against our coalition forces.

LT. CRAGG: Sir, do you want to elaborate? Does anybody else have any other questions as well? (No response.)

COL. PARKS: If not, we'll leave it up for any more questions. If there's anything else in the area of electronic warfare, that might   be helpful for what we're trying to help you all understand about the Combined Arms Center and what we're doing.

Q   Yeah, I'm good. Thanks.

LT. CRAGG: With that, sir, gentlemen, if you would like to close with a closing statement, if you want to go further into any subject matter as a closing statement, feel free to do so.

COL. PARKS: Yeah, I think I just want to thank you guys again for the opportunity. The questions you're asking are really fantastic. You know, I have a crew here that sits and writes your questions down. And in all cases, I can't say that we've thought that through carefully enough or had enough time to do that, certainly is is that your questions pose a whole series of other questions for us that we will take away and go back and start working on.

And I didn't -- I don't mean to cut anybody off here.

But I want to make sure that I reiterate that what we've done in the United States Army in our current doctrine is we have taken the area of cognitive, humanities, social sciences type capability development and we've really focused in on that because that -- you know, operating in and amongst the population on the ground in a human-to-human context is always going to be key to our success or not success within the United States Army, and especially with us -- boots on the ground all the time.

On the other hand is, is you've got this piece that I'm working on, which is more of the technical nature or, as I've said, natural and formal sciences, computer sciences and being able to put a focus and emphasis on that. And that's what I'm doing within the Computer Network Operations and Electronic Warfare Proponent in trying to really put some intellectual rigor behind what I'm calling right now cyberelectronics and making sure we understand the natural phenomena associated with that and how our physical capabilities are going to be able to impact that over time.

I do owe an answer on -- I keep using the term self-healing. And I'm afraid it escapes me on the actual term I'm looking for, but I'll get that and I'll send it back out to the folks there at the DOD Blogger Roundtable and give you a better explanation, or by all means feel free to come to our website and ask us some questions. We'll be glad to answer those directly.

Q Is it neural networks?

COL. PARKS: That's not the term, but you've got the idea.

LT. CRAGG: And so for anybody who's listening who didn't attend this call, can you cite that website?

COL. PARKS: Yes. Hang on just a second, please. Let me give you the exact name. Okay, you can access the Combined Arms Center at www.leavenworth.army.mil. And when you come there, you'll see the Combined Arms Center -- Lieutenant General Caldwell's website. And one of the subordinate organizations is the CNO and Electronic Warfare proponent. And once you get to that site there's other links out to blog sites that we use and other sites that we're connected to virtually, that -- you can always send a question to us through that site or you can see the kinds of things that we're doing in those different places that we're connected to in order to do our work. LT. CRAGG: And any of the bloggers on the call, if you have any follow-on questions about any of the topics discussed, you can shoot them to me and I'll make sure that I send them out to Lieutenant Colonel Harper and then, as well, Colonel Parks.

Sir, gentlemen and -- thank you for attending today's Bloggers Roundtable, as well as the bloggers. All of the information -- the audio file and the bio will be available on the bloggers link on dod.mil. Again, thank you, gentlemen, for joining today's call. I appreciate it.

And this concludes today's event, if there's not any last-minute questions. Everything's good to go?

COL. PARKS: Yeah.

Q Colonel, thanks very much. Appreciate the time today.

Q Thank you, Colonel.

LT. CRAGG: Thank you, sir. END.